What Is Claimed Is:

1. A data storage device provided with a function for authenticating a user's access right, which verifies legitimacy of proof data generated for proving a right of an application program to access data stored in a storage medium, to thereby authenticate the access right of a user of the application program to the data, the data storage device comprising:

first storage means for storing authentication data;

second storage means for storing user unique identifying information of the user of the application program;

third storage means for storing auxiliary proof information being a result in which a specific calculation is executed to the user unique identifying information of the application program and unique security characteristic information;

proof data generation means for executing a specific calculation to the authentication data stored in the first storage means, the user unique identifying information of the application program stored in the second storage means, and the auxiliary proof information stored in the third storage means, to thereby generate proof data;

a data storage main frame provided with a storage medium, which stores and preserves data in the storage medium;

command generation means installed in the application program, for generating a command that instructs an operation to the data stored in the storage medium of the data storage main frame;

command issuing means installed in the application program, for issuing the command generated by the command generation means to the outside of the application program;

proof data verification means for verifying that the proof data generated by the proof data generation means has been generated on the basis of the unique security characteristic information; and

command management means for permitting to execute the command only when the verification is successful, as to at least one type of the command that instructs the operation to the data stored in the data storage main frame.

2. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein at least the second storage means and the proof data generation means are retained in protection means for making it difficult to observe the inner data and processing procedures from the outside.

3. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein at least the second storage means and the proof data generation means are configured in a small portable processor such as an IC card.

4. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein the proof data generation means includes first calculation means and second calculation means, in which the first calculation means executes a specific calculation to the user unique identifying information of the application program stored in the second storage means and the auxiliary proof information stored in the third storage means to produce the unique security characteristic information as a result of the calculation, and the second calculation means executes a specific calculation to the authentication data stored in the first storage means and the unique security characteristic information calculated by the first calculation means to generate the proof data as a result of the calculation.

5. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, in which the third calculation means executes a specific calculation to the authentication data stored in the first storage means and the auxiliary proof information stored in the third storage means, the fourth calculation means executes a specific calculation to the authentication data stored in the first storage means and the user unique identifying information of the application program stored in the second storage means, and the fifth calculation means executes a specific calculation to a calculation result by the third calculation means and a calculation result by the fourth calculation means, to generate the proof data as a result of the calculation.

6. A data storage device provided with a function for authenticating a user's access right according to Claim 5, wherein at least the second storage means and the fourth calculation means are retained in protection means for making it difficult to observe the inner data and processing procedures from the outside.

7. A data storage device provided with a function for authenticating a user's access right according to Claim 5, wherein at least the second storage means and the fourth calculation means are configured in a small portable processor such as an IC card.

8. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein the unique security characteristic information is a decryption key in an encryption function, the authentication data is appropriate data encrypted by using an encryption key corresponding to the decryption key, and the proof

data verification means verifies that the proof data generated by the proof data generation means is identical to the correct decryption of the authentication data.

9. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein the unique security characteristic information is an encryption key in an encryption function, and the proof data generated by the proof data generation means is verified to be the authentication data correctly encrypted by using the encryption key.

10. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein the unique security characteristic information is a signature key in a digital signature function, and the proof data generated by the proof data generation means is verified to be a digital signature to the authentication data generated by using the signature key.

11. A data storage device provided with a function for authenticating a user's access right according to Claim 8, wherein the encryption function is an asymmetric encryption function, and the unique security characteristic information is a key on one side.

12. A data storage device provided with a function for authenticating a user's access right according to Claim 11, wherein the encryption function is a public key encryption function, and the unique security characteristic information is a private key.

13. A data storage device provided with a function for authenticating a user's access right according to Claim 8, wherein the encryption function is a symmetric

encryption function, and the unique security characteristic information is a common secret key.

14. A data storage device provided with a function for authenticating right of the user of an application program to access data, through mutual communication between a proof data generation device including the first storage means, the second storage means, the third storage means, and the proof data generation means, and a proof data verification device including, in addition to the proof data verification means, fourth storage means for storing the authentication data and fifth storage means for storing the proof data, according to Claim 1, wherein the proof data verification device writes the authentication data stored in the fourth storage means into the first storage means of the proof data generation device, the proof data generation device writes the proof data generated on the basis of the authentication data written into the first storage means by the proof data generation means into the fifth storage means of the proof data verification device, and the proof data verification device authenticates the user's access right by using the proof data written into the fifth storage means.

15. A data storage device provided with a function for authenticating a user's access right according to Claim 14, wherein the unique security characteristic information is an encryption key in an encryption function, the proof data verification device includes random number generation means, the random number generation means writes a random generated number into the fourth storage means as the authentication data, and the proof data verification means verifies the proof data written into the fifth storage means by the proof data generation device to be the encryption of the random number being the authentication data using encryption key being the unique security characteristic information.

16. A data storage device provided with a function for authenticating a user's access right according to Claim 14, wherein the unique security characteristic information is a decryption key in an encryption function, the proof data verification device includes random number generation means, sixth storage means for storing a generated random number, and seventh storage means for storing a seed for authentication data, the random number generation means writes a generated random number into the sixth storage means, randomizes the seed for authentication data stored in the seventh storage means by using the random number, and thereafter writes the result of the randomization as the authentication data into the fourth storage means, and the proof data verification means verifies the result with the random number effect by the random number stored in the sixth storage means removed from the proof data written into the fifth storage means to be identical to the decryption of the seed for authentication data stored in the seventh storage means by the decryption key being the unique security characteristic information.

17. A data storage device provided with a function for authenticating a user's access right according to Claim 14, wherein the unique security characteristic information is a signature key in a digital signature function, the proof data verification device includes random number generation means, the random number generation means writes a generated random number into the fourth storage means as the authentication data, and the proof data verification means verifies the proof data written into the fifth storage means by the proof data generation device to be a digital signature to the authentication data being the random number by the signature key being the unique security characteristic information.

18. A data storage device provided with a function for authenticating a user's access right according to Claim 15, wherein the encryption function is of the RSA public

key crypto-system using a modulus n, the unique security characteristic information is a private key D, a public key corresponding to the private key D is E, and the proof data verification means verifies E power of proof data R written into the fifth storage means to be congruent with an authentication data C stored in the fourth storage means, modulo n ($R^E \bmod n = C \bmod n$).

19. A data storage device provided with a function for authenticating a user's access right according to Claim 16, wherein the encryption function is of the RSA public key crypto-system using a modulus n, the unique security characteristic information is a private key D, a public key corresponding to the private key D is E, the seed for authentication data stored in the seventh storage means is a number K' being E power of a data K modulo n ($K' = K^E \bmod n$), the random number generation means writes a number C being E power of a random number r modulo n multiplied by the number K' modulo n ($C = r^E K' \bmod n$) into the fourth storage means as the authentication data, and the proof data verification means verifies a reverse modulo n of the random number r stored in the sixth storage means multiplied by proof data R written into the fifth storage means to be congruent with the data K modulo n ($K \bmod n = r^{-1}R \bmod n$).

20. A data storage device provided with a function for authenticating a user's access right according to Claim 18, wherein the encryption function is of the RSA public key crypto-sustem using a modulus n, the unique security characteristic information is the private key D, the public key corresponding to the private key D is E, auxiliary proof information t stored in the third storage means is data obtained by subtracting user unique identifying information e of the application program stored in the second storage means from the private key D, and adding a product of a value of a non-collision function ω (= G(n, e)) dependent on the modulus n and the user unique identifying information e, and an Eulerian number $\phi(n)$ ($t = D - e + \omega\phi(n)$), and the proof data generation means

generates the proof data by calculating D power of C modulo n (C^D mod n), from the t, the e, and the authentication data C stored in the first storage means.

21. A data storage device provided with a function for authenticating a user's access right according to Claim 20, wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, the third calculation means calculates the t power of the C modulo n (C^t mod n), the fourth calculation means calculates the e power of the C modulo n (C^e mod n), and the fifth calculation means multiplies a result of the calculation by the first calculation means by that of the calculation by the second calculation means modulo n to thereby generate the proof data R ($=C^tC^e$ mod n).

22. A data storage device provided with a function for authenticating a user's access right according to Claim 21, wherein the second storage means and the fourth calculation means are built in protection means for protecting the inner processing procedures and data from outside observation.

23. A data storage device provided with a function for authenticating a user's access right according to Claim 18, wherein the encryption function is of the RSA public key crypto-system using a modulus n, the unique security characteristic information is the private key D, the public key corresponding to the private key D is E, auxiliary proof information t stored in the third storage means is data obtained by adding to the D a value of a non-collision function F(n, e) which is dependent on the modulus n and user unique identifying information e of the application program stored in the second storage means (t = D + F(n, e)), and the proof data generation means generates the proof data by calculating D power of C modulo n (C^D mod n), from the t, the e, and the authentication data C stored in the first storage means.

24. A data storage device provided with a function for authenticating a user's access right according to Claim 23, wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, the third calculation means calculates the t power of the C modulo n (C^t mod n), the fourth calculation means calculates the F(n, e) power of the C modulo n ($C^{F(n, e)}$ mod n), and the fifth calculation means multiplies a result of the calculation by the third calculation means by the reverse of a calculation result by the fourth calculation means modulo n to thereby generate the proof data R ($=C^tC^{-F(n, e)}$ mod n).

25. A data storage device provided with a function for authenticating a user's access right according to Claim 24, wherein the second storage means and the fourth calculation means are built in protection means for protecting the inner processing procedures and data from outside observation.

26. A data storage device provided with a function for authenticating a user's access right according to Claim 15, wherein the encryption function is of the Pohlig-Hellman asymmetric crypto-system using a modulus p, the unique security characteristic information is a key D on one side, a key on the other side corresponding to the key D is E (DE mod p-1 = 1), and the proof data verification means verifies E power of proof data R written into the fifth storage means to be congruent with authentication data C stored in the fourth storage means, modulo p (R^E mod p = C mod p).

27. A data storage device provided with a function for authenticating a user's access right according to Claim 16, wherein the encryption function is of the Pohlig-Hellman asymmetric crypto-system using a modulus p, the unique security characteristic information is a key D on one side, a key on the other side corresponding to the key D is

E (DE mod p-1 = 1), the seed for authentication data stored in the seventh storage means is a number K' being E power of a data K modulo p ($K' = K^E \bmod p$), the random number generation means writes a number C that is identical to E power of a random number r modulo p multiplied by the number K' modulo p ($C = r^E K' \bmod p$) into the fourth storage means as the authentication data, and the proof data verification means verifies a reverse modulo p of the random number r stored in the sixth storage means multiplied by the proof data R written into the fifth storage means to be congruent with the data K modulo p ($K \bmod p = r^{-1} R \bmod p$).

28. A data storage device provided with a function for authenticating a user's access right according to Claim 26, wherein the encryption function is of the Pohlig-Hellman asymmetric crypto-system using a modulus p, the unique security characteristic information is a key D on one side, a key on the other side corresponding to the key D is E (DE mod p-1 = 1), auxiliary proof information t stored in the third storage means is data obtained by adding to the D a value of a non-collision function F(p, e) which is dependent on the modulus p and user unique identifying information e of the application program stored in the second storage means (t = D + F(p, e)), and the proof data generation means generates the proof data by calculating D power of C modulo p ($C^D \bmod p$), from the t, the e, and the authentication data C stored in the first storage means.

29. A data storage device provided with a function for authenticating a user's access right according to Claim 28, wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, the third calculation means calculates the t power of the C modulo p ($C^t \bmod p$), the fourth calculation means calculates the F(p, e) power of the C modulo p ($C^{F(p, e)} \bmod p$), and the fifth calculation means multiplies a result of the calculation by the third calculation

means by the reverse of a calculation result by the fourth calculation means modulo p to thereby generate the proof data R ($=C^{t}C^{-F(p, e)} \bmod p$).

30. A data storage device provided with a function for authenticating a user's access right according to Claim 29, wherein the second storage means and the fourth calculation means are built in protection means for protecting the inner calculation procedures and data from outside observation.

31. A data storage device provided with a function for authenticating a user's access right according to Claim 16, wherein, when the encryption function is of the ElGamal public key crypto-system using a modulus p of the ElGamal public key crypto-system using a modulus p and a generator a, the unique security characteristic information is a private key X, a public key corresponding to the key X is Y ($Y = a^{X} \bmod p$), u is a number that the a is exponentiated by an appropriate random number z as an exponent modulo p ($u = a^{z} \bmod p$), and K' is a product of data K and the Y exponentiated by the random number z modulo p ($K' = Y^{z}K \bmod p$), a combination of the u and the K' is stored in the seventh storage means as the seed for authentication data, the random number generation means writes the u and a number C that results from a random number r multiplied by the number K' modulo p ($C = rK' \bmod p$) into the fourth storage means as the authentication data, and the proof data verification means verifies a reverse modulo p of the random number r stored in the sixth storage means multiplied by proof data R written into the fifth storage means to be congruent with the data K modulo p ($K \bmod p = r^{-1}R \bmod p$).

32. A data storage device provided with a function for authenticating a user's access right according to Claim 31, wherein, when the encryption function is of the ElGamal public key crypto-system using a modulus p and a generator a, the unique

security characteristic information is a key X on one side, a public key corresponding to the key X is Y ($Y = a^X \bmod p$), auxiliary proof information t stored in the third storage means is data obtained by adding to the X a value of a non-collision function F(p, e) which is dependent on the modulus p and user unique identifying information e of the application program stored in the second storage means ($t = X + F(p, e)$), and the proof data generation means generates the proof data by calculating C divided by X power of the u modulo p ($Cu^{-X} \bmod p$), from the t, the e, and the authentication data u and C stored in the first storage means.

33. A data storage device provided with a function for authenticating a user's access right according to Claim 32, wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, the third calculation means calculates the t power of the u modulo p ($u^t \bmod p$), the fourth calculation means calculates the F(p, e) power of the u modulo p ($u^{F(p, e)} \bmod p$), and the fifth calculation means divides the C by a calculation result of the third calculation means modulo p and multiplies a calculation result of the fourth calculation means to thereby generate the proof data R ($=Cu^{-t}\, u^{F(p, e)} \bmod p$).

34. A data storage device provided with a function for authenticating a user's access right according to Claim 33, wherein the second storage means and the fourth calculation means are built in protection means for protecting the inner calculation procedures and data from outside observation.

35. A data storage device provided with a function for authenticating a user's access right according to Claim 17, wherein the digital signature function is of the ElGamal sgnature scheme using the modulus p and a generator a, the unique security characteristic information is a signature key X, a public key corresponding to the key X

is Y ($Y = a^X \bmod p$), and the proof data verification means verifies, in regard to a proof data R and S, a value being the a exponentiated by authentication data C as an exponent stored in the fourth storage means, modulo p to be congruent with a product of the R power of the Y and the S power of the R, modulo p ($a^C \bmod p = Y^R R^S \bmod p$).

36. A data storage device provided with a function for authenticating a user's access right according to Claim 35, wherein the digital signature function is the E1Gamal signature under the modulus p and a generator a, the unique security characteristic information is the signature key X, the public key corresponding to the key X is Y ($Y = a^X \bmod p$), auxiliary proof information t stored in the third storage means is data obtained by adding to the X a value of a non-collision function F(p, e) which is dependent on the modulus p and a user unique identifying information e of the application program stored in the second storage means ($t = X + F(p, e)$), and the proof data generation means generates an appropriate random number k in generating the proof data R and S, adopts the k power of the a modulo p as the R ($= a^k \bmod p$), subtracts a product of the X and the R from the C modulo p-1 and multiplies the calculation result with a reverse of the k, from the t, the e, and the authentication data C written into the first storage means, and thereby calculates the S ($= (C-RX)k^{-1} \bmod p-1$).

37. A data storage device provided with a function for authenticating a user's access right according to Claim 36, wherein the second storage means and the proof data generation means are built in protection means for protecting the inner calculation procedures and data from outside observation.

38. A data storage device provided with a function for authenticating a user's access right according to Claim 4, wherein the user unique identifying information of the application program is a decryption key of an encryption function, the auxiliary proof

information is the unique security characteristic information encrypted by an encryption key corresponding to the decryption key, and the first calculation means decrypts the auxiliary proof information by using the decryption key being the user unique identifying information of the application program to thereby calculate the unique security characteristic information.

39. A data storage device provided with a function for authenticating a user's access right according to Claim 38, wherein the encryption function is an asymmetric key encryption function, and the user unique identifying information of the application program is a key on one side.

40. A data storage device provided with a function for authenticating a user's access right according to Claim 39, wherein the encryption function is a public key encryption function, and the user unique identifying information of the application program is a private key.

41. A data storage device provided with a function for authenticating a user's access right according to Claim 38, wherein the encryption function is a symmetric key encryption function, and the user unique identifying information of the application program is a common secret key.

42. A data storage device provided with a function for authenticating a user's access right according to Claim 8, wherein the proof data verification means includes eighth storage means for storing clear text data corresponding to the authentication data or the seed for authentication data being encrypted data and comparison means, and the comparison means compares the proof data generated by the proof data generation means or a result having the random number effect removed from the proof data with the

clear text data stored in the eighth storage means, and only when both are identical, judges the proof data to be legitimate.

43. A data storage device provided with a function for authenticating a user's access right according to Claim 8, wherein the proof data verification means includes ninth storage means for storing a result having a specific one-way function applied to clear text data corresponding to the authentication data or the seed for authentication data being encrypted data, sixth calculation means, and comparison means, the sixth calculation means applies the one-way function to the proof data generated by the proof data generation means after derandomizing if necessary, and the comparison means compares a calculation result by the sixth calculation means with data stored in the ninth storage means, and only when both are identical, judges the proof data to be legitimate.

44. A data storage device provided with a function for authenticating a user's access right according to Claim 8, wherein the proof data verification means includes program execution means, the authentication data or the seed for authentication data is data obtained by encrypting a program, the proof data verification means passes, after derandomizing if necessary, the proof data generated by the proof data generation means to the program execution means as a program, whereby the program execution means executes a correct operation, when the proof data generation means correctly decrypts the authentication data or the seed for authentication data being an encrypted program, namely, only when the encrypted program is correctly decrypted.

45. A data storage device provided with a function for authenticating a user's access right according to Claim 8, wherein the proof data verification means includes program execution means, program storage means, and program decryption means, a program stored in the program storage means is encrypted to a part or whole thereof, the

authentication data or the seed for authentication data is data obtained by separately encrypting a decryption key for decrypting the encrypted program, the proof data verification means passes the proof data generated by the proof data generation means to the program decryption means, the program decryption means uses, after derandomizing if necessary, the proof data generated by the proof data generation means as a decryption key to thereby decrypt a necessary part of the program stored in the program storage means, the program execution means executes the decrypted program, whereby, when the proof data generation means correctly decrypts the authentication data or the seed for authentication data, namely, only when the decryption key for decrypting the encrypted program is correctly decrypted, the program execution means executes a correct operation.

46. A data storage device provided with a function for authenticating a user's access right according to Claim 14, wherein the proof data generation device and the proof data verification device are installed in one enclosure, and the proof data generation device and the proof data verification device communicate with each other without using a communication medium outside the enclosure.

47. A data storage device provided with a function for authenticating a user's access right, which verifies legitimacy of proof data generated for proving right of an application program to access data, stored in a storage medium, to thereby authenticate the access right of a user of the application program to the data, the data storage device comprising:

first storage means for storing authentication data;

second storage means for storing user unique identifying information of the application program;

third storage means for storing auxiliary proof information being a result in which a specific calculation is executed to the user unique identifying information of the application program and unique security characteristic information;

proof data generation means for executing a specific calculation to the authentication data stored in the first means and the user unique identifying information of the application program stored in the second storage means, to thereby generate proof data;

a data storage main frame provided with a storage medium, which stores and preserves data in the storage medium;

command generation means installed in the application program, for generating a command that instructs an operation to the data stored in the storage medium of the data storage main frame;

command issuing means installed in the application program, for issuing a command generated by the command generation means to the outside of the application program;

proof data verification means including calculation means for applying a specific calculation to the proof data generated by the proof data generation means and the auxiliary proof information held in the third storage means, which verifies the proof data to be generated on the basis of the user unique identifying information of the application program, by using a calculation result by the calculation means; and

command management means for permitting to execute the command only when the verification is successful, as to at least one type of the command that instructs the operation to the data stored in the data storage main frame.

48. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein the storage medium of the data storage device is a write once optical storage medium.

49. A data storage device provided with a function for authenticating a user's access right according to Claim 48, wherein the write once optical storage medium of the data storage device is a phase change type optical storage medium.

50. A data storage device provided with a function for authenticating a user's access right according to Claim 48, wherein the write once optical storage medium of the data storage device is a phase separation type optical storage medium.

51. A data storage device provided with a function for authenticating a user's access right according to Claim 1, wherein the storage medium that first stores at least a specific access log, of the storage medium of the data storage device, is a write once optical storage medium.

52. A data storage device, comprising a write once optical storage medium that is used for a part that first stores a specific access log as auxiliary storage means.